Notice of Allowability	Application No.	Applicant(s)	
	09/386,341	INADA, RYU	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *03 June 2004*.

2. ☒ The allowed claim(s) is/are *1-6,8-13 and 15-19*.

3. ☒ The drawings filed on *31 August 1999* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

THOMAS R. PEESO
PRIMARY EXAMINER

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mrs. Randi B. Isaacs, Registration No. 56,046, on November 23, 2004.

The application has been amended as follows:

1. In claims 9 and 29, in line 6, change "signature, an encrypted signature..." to "signature, and an encrypted signature..."

2. Delete the following from claims 9 and 19, in lines 7-9 and 7-10, respectively:

", said encrypted private key, said encrypted common key, said second public key, and a signature written by use of said signature private key on said encrypted signature private key"

3. Cancel claim 14

4. In claim 15, line 7, change "said lock data" to "a lock data"

5. In claim 16, line 10, change "in said lock" to "in a lock"

6. In claim 17, line 9, change "in said lock" to "in a lock"

Allowable Subject Matter

Claims 1-6, 8-13 and 15-19 are allowed.

The following is an examiner's statement of reasons for allowance:

The primary reasons for the allowance of the independent claims 1, 3-6, 9 and 15-19 are the inclusion of the following limitations that are not found in the prior art and they are uniquely distinct features. The closest prior art are Okamoto et al (6,118,874) and Langford et al (6,266,420 B1). Okamoto et al discloses a key recovery system that generates an enveloped data by combining an encrypted plaintext generated by using a common key and encrypted said common key(s) generated by using the public keys of the members of a group. Langford teaches a method for a secure group communication, where the group communication is secured based on the security credentials of the group. However, These two arts, singularly or in combination, fail to anticipate or render the following limitation:

"Claims 1 and 3: storing lock data which includes a group public key, an encrypted private key formed by encrypting a group private key that corresponds to said group public key, by use of a common key, and a plurality of encrypted common keys generated by encrypting said common key by use of respective public keys of the group members".

"Claim 4: storing lock data which includes a group public key, an encrypted private key, the encrypted private key being formed by encrypting a group private key that corresponds to said public key, by use of a common key, and a plurality of encrypted common keys generated by encrypting said common key by use of respective public keys of the group members".

"Claim 5: encrypting said common key by use of public keys of respective group members to generate corresponding encrypted common key; and

combining said public keys, said encrypted private key, and said encrypted common keys to generate lock data".

"Claim 6: modifying said group private key by use of a desired function including an inverse function to generate a modified group private key;

encrypting said common key by use of public keys of respective group members to generate corresponding encrypted common key; and

combining said public keys, said encrypted private key, and said encrypted common keys to generate lock data".

"Claim 9: storing lock data including a first public key, an encrypted private key formed by encrypting a private key corresponding to said first public key by use of a common key, a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group members, a second public key for verifying a signature, and an encrypted signature private key formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder".

"Claims 15-17: a memory part that stores a group public key, an encrypted private key formed by encrypting a group private key corresponding to said group public key, by use of a common key, and a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group members".

"Claim 18: a generation part that encrypts said group private key by use of said common key to generate an encrypted private key;

a generation part that encrypts said common key by use of public keys of respective group members to generate an encrypted common key; and

a generation part that combines said group public key, said encrypted private key, and said encrypted common key to generate lock data".

"Claim 19: a memory part that stores lock data including a first public key, an encrypted private key formed by encrypting a private key corresponding to said first public key by use of a common key, a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective group members, a second public key for verifying a signature, and an encrypted signature private key formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder".

The dependent claims 2, 8 and 10-13 are allowed because they were originally found to include a unique feature not found in the closest abovementioned art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

A.N.

AN

November 24, 2004

THOMAS R. PEESO
PRIMARY EXAMINER